A Publication of the DCIS Northeast Field Office

TECHNOBABBLE

The DCIS Cyber Crime Newsletter

TECHNOBABBLE
Volume 2, Issue 4

July, 2001

This issues suggested computer crime bookmarks:

Packet Storm Internet Security Page:

http://www.packetstorm.securify.com

Anti-online Security Page:

http://www.antionline.com

Insecure Security Page:

http://www.insecure.org

Inside this issue:

Former DoD Police Officer Indicted 1

Hacker Crashes Entire Nation. 1

Identifying System Vulnerabilities with Nessus. 2

Know the Code! 18 USC 1030. 4

Suggested Reading: “The Cuckoo’s Egg.” 5

Former DoD Police Officer Indicted

On June 14, 2001, Miguel A. Garcia, a former DoD Police Officer previously assigned to the U.S. Army Military Ocean Terminal, Bayonne (MOTBY), NJ, and Ft. Monmouth, NJ, was indicted in the Southern District of New York on the following charges: Forgery of Seals of Departments or Agencies; Forgery of Official Badges, Identification Cards; False Statements; and Mail Fraud.

The indictment alleges that Garcia was in possession of parking placards bearing the seals and insignias of various United States Departments and Agencies (including those of the Department of Defense), and in possession of equipment and materials for manufacturing and laminating official Government parking placards. It is also alleged that Garcia sold two United States Marshals' Service shields to unauthorized persons and made false statements regarding those sales to investigating agents.

If convicted Garcia faces up to 30 years incarceration.

The investigation provides yet another example of how advances in technology have created opportunities for abuse. It is alleged that Garcia utilized computer equipment in conjunction with other readily available items to create the referenced seals, identification cards, and placards.

The investigation was conducted by the Defense Criminal Investigative Service’s New York Resident Agency in conjunction with the Law Enforcement Integrity Unit of the U.S. Attorney's Office, Southern District of New York, the Federal Bureau of Investigation, the New York State Inspector General's Office, and the New York State Commission of Investigation.

Hacker Crashes Entire Nation

Reprinted from World Entertainment News Network, July 3, 2001

A computer whizzkid has been fined £2,000 ($2,600) for hacking into the United Arab Emirates' only internet provider and causing the whole country's system to crash. Lee Ashurst, 22, originally from Oldham in Greater Manchester, England, was convicted of misusing equipment, services or facilities provided by Emirates Telecommunications Corp Etisalat.

Ashurst, who works for a construction company in the Gulf, is now facing a compensation claim of more than £500,000 ($650,000) from Etisalat after the Dubai Court of First Instance transferred his case to the civil courts. He was working as a computer engineer at a Dubai construction firm in May last year (00) when he began hacking into Etisalat's systems.

According to the Gulf News newspaper, the court was told the entire United Arab Emirates internet system crashed on several occasions over a month.

Identifying System Vulnerabilities with Nessus

By Special Agent Jim Ives, DCIS Boston Resident Agency

Ask any system administrator and they will tell you that keeping their systems secure from hackers and internal misuse requires constant vigilance. New security vulnerabilities are discovered on a regular basis, and hackers are more than willing to utilize these vulnerabilities to their advantage. Compounding the problem is the fact that most sysadmins spend the majority of their days (and oftentimes, their nights) fighting to keep their systems up and running, addressing users' concerns, and handling day to day anomalies and glitches which are common to any network.

So how can a sysadmin pressed for time effectively audit their network for potential security vulnerabilities? Luckily, automated tools, such as security scanners, are available to sysadmins to help them to identify potential problems, and to subsequently "harden" their systems.

WHAT IS A SECURITY SCANNER?

Simply put, a security scanner is software which will audit a given computer network, and report whether various system vulnerabilities exist. Upon identifying potential security issues, more advanced scanners will provide direction as to how the vulnerability can be eliminated. Unfortunately, over the years, some security scanners have developed nasty reputations. Many of these scanners are freely available on the Internet, and since these scanners can be utilized to audit systems remotely, they have become useful tools in hackers' arsenals. In fact, one of the first steps hackers generally take in attempting to break into computer systems is to scan the network of interest in order to ascertain whether known vulnerabilities exist. One such scanner, known as NMAP, is so common that a search of any hackers' computer system will almost assuredly identify a copy of the program. Fortunately, most modern day firewalls (when properly configured) can block these scans, and most Intrusion Detection Systems (IDS) will alert administrators to the fact that their system is being scanned. Unfortunately, newer version of scanners can be configured to defeat certain firewalls (especially if misconfigured). It is also unfortunate that the prevalence of scanning (leave a system on-line for any period of time, and it will most assuredly be scanned by a hacker with a bit too much time on his hands) has resulted in many administrators simply ignoring IDS reports of scanning activity.

THE NESSUS PROJECT

In 1998, a group of programmers led by Jordan Hrycaj and Renaud Deraison set out to create a security scanner which was thorough, simple to use, and (of significant importance to cash strapped organizations) - free of charge. Deraison, via the Nessus website (www.nessus.org) indicates that at the time of initial release, the only thorough and free security scanner available was SATAN (Security Administrator Tool for Analyzing Networks), and due to lack of continued development of the utility, the tool became outdated. The project has been incredibly successful, and Nessus is now recognized as one of the most thorough tools available to audit systems security. Through constant updating of security scripts which identify new vulnerabilities (known as "plugins") utilized by the Nessus engine, which are allegedly updated daily, the creators of Nessus have created a utility which will maintain its usefulness.

DOWNLOADING NESSUS

Nessus consists of two separate modules - a server (nessusd) which is responsible for the attacks, and a client which collects the results. Although there are three clients available (one for the Gimp Tool Kit, one for Microsoft Windows, and one for Java), there is only one version of the server (for POSIX systems: i.e. Linux, Solaris, FreeBSD, etc.). For the sake of simplicity, we will assume a standard Linux install. Successfully installing the scanner does require that certain items be present on your system: namely, The Gimp Toolkit version 1.2 (available at `ftp://ftp.gimp.org/pub/gtk/v1.2.`), NMap (`available at http://www.insecure.org/nmap` - version 2.52 is recommended), and m4 if your system does not come installed with a libgmp (available at `ftp.gnu.org/pub/gnu/m4`). Assuming these utilities are present on your system, you are ready to download and compile the required packages. **The following four packages must be downloaded and compiled in the listed order, otherwise the installation is likely to fail:**

- nessus-libraries

> *"Luckily, automated tools, such as security scanners, are available to sysadmins to help them to identify potential problems, and to subsequently 'harden' their systems."*

- libnas1
- nessus-core
- nessus-plugins

A list of several FTP sites offering the packages can be found at: `http://www.nessus.org/posix.html`. Look for the files: `nessus-libraries-x.x.tar.gz` , `libnasl-x.x.tar.gz` , `nessus-core.x.x.tar.gz` , and `nessus-plugins.x.x.tar.gz`. Once you have downloaded these files, you are ready to compile for use on your system.

COMPILING & INSTALLING NESSUS

Compiling and installing the program is fairly straight forward, but remember, you have to install the packages in order. Untar each of the files. This will create separate directories. From the command prompt, type :

```
cd nessus-libraries
./configure
make
```

After this, execute this command as root :

```
make install
```

"Keep in mind that no single utility can ever detect each and every vulnerability which could potentially threaten a system."

Then, compile and install the next library:

```
cd libnasl
./configure
make
```

And as root, execute the command:

```
make install
```

Repeat the same operation with nessus-core and nessus-plugins.

Also, make sure that `/usr/local/lib` is in `/etc/ld.so.conf`. If it isn't, modify the file, and from the command prompt type: `ldconfig`.

Assuming the install was successful, you will now need to create a nessusd (the nessus server) account. The nessus-adduser command will accomplish this goal. From the command prompt, type: nessus-adduser. The session should look similar to the following:

```
$ nessus-adduser

Login : Jives <user defined>
Password : dcis <user defined>
Authentification type
(cipher or plaintext)
[cipher] : <enter>

Now enter the rules for
this user, and hit ctrl-D
once you are done :
the user can have an empty
rule set) : <enter>

Login              : JIves
Pssword            : dcis
Authentification : cipher
Rules              :

Is that ok (y/n) ? [y] y
user added.
```

Next, you will have to start the Nessus client. Accomplish this be typing:

```
nessusd -D
```

Assuming all has gone as planned, you should now be ready to use Nessus.

USING NESSUS

The first step in using Nexxus is launching the client front-end. At the command prompt, type `nessus`, and program should execute. The graphical user interface will appear. Immediately click on the 'log in' option, and enter the password you supplied when initially setting up the server account. You should then be logged on. The folders located at the top of the screen will let you configure the scan to your liking. You may wish to be selective (be especially careful with some of the denial of service scans, as they may cause crashes), or you may simply wish to run a full scan for all known vulnerabilities. For specifics relative to setting up configurations, see `www.nessus.org/demo/second.html`. Once you have configured to your liking, choose the 'Target Selection' option, and enter the IP address or domain of the system you wish to scan. Then, choose the 'Start the Scan' option at the bottom of the user interface. Depending upon the configuration you chose, the scan may take quite some time to complete. However, when the scan has been completed, a 'test result' window will appear which contains a thorough report detailing vulnerabilities which were identified, as well as suggestions as to how to correct the vulnerabilities, and URL's which can be accessed in order to receive more information.

A WORD OF WARNING

Keep in mind that no single utility can ever detect each and every vulnerability which could potentially threaten a system. Utilization of scanners such as Nessus is but one of many security audit routines that a system administrator may wish to periodically employ. Also keep in mind that you should never scan a system for vulnerabilities without the express consent of individuals responsible for said system. Scans such as those accomplished via Nessus are generally **very** obvious to even the most elementary IDS systems, and scans of the nature performed by Nessus can significantly degrade performance of the target system, or in limited instances, even crash the system. Although scans of systems are not illegal per se, you should only scan systems within sole intent of identifying and correcting vulnerabilities.

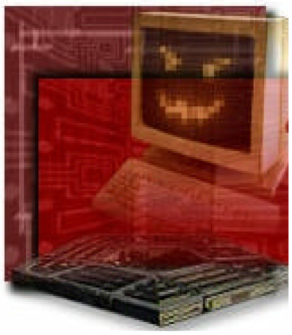
CONCLUSION

With the limited time available to most system administrators, automated tools such as vulnerability scanners can provide an effective means to periodically assess the security of their systems. Although often thought of as the tools of hackers, in reality, scanners such as Nessus can function as a first line of defense against those who are inclined to illegally access and misuse your systems.

For more information, see:

`http://www.nessus.org`

NOTE: Neither the author nor DCIS makes any representations or warranties relative to the products referenced within this article. In no event will DCIS be liable for any indirect, punitive, special, incidental, or consequential damages, however they may arise relative to the use of products referenced within this article. There are inherent dangers in the use of any software available for download on the Internet, and the author cautions you to make sure that you completely understand the potential risks before downloading any of the software, or utilizing the software on your system. Should you choose to download and utilize the referenced application, you are solely responsible for adequate protection and backup of the data and equipment used in connection with any of the software, and neither the author nor DCIS will be held liable for any damages that you or your organization may suffer in connection with using, modifying or distributing any of the software referenced herein.



Know the Code!

Common Federal Statutes Utilized in Prosecuting Computer Crime

By Special Agent Jim Ives, DCIS Boston Resident Agency

18 USC 1030–Fraud and Related Activity in Connection with Computers

This article will be the first of several which explores various federal statutes utilized in prosecuting computer related crimes. Although computer crime investigators and prosecutors are generally familiar with these statutes, systems administrators and network security professionals are rarely given the opportunity to review and digest information relative to the statutes which investigators and attorneys use on a daily basis to combat computer related crime.

The statute most commonly utilized in connection with prosecuting computer crime at the federal level is Title 18 United States Code, Section 1030, entitled “Fraud and Related Activity in Connection with Computer Crime.” Although the statute has been referred to as “the hacker statute” throughout the law enforcement community, it actually contains language which could be utilized to prosecute several types of computer-related crime, including internal misuse of computer systems, introduction of viruses into protected systems, and denial of service attacks.

> *“...it actually contains language which could be utilized to prosecute several types of computer-related crimes, including internal misuse of computer systems, introduction of viruses into systems, and denial of service attacks.”*

The full text of the statute is as follows:

(a) Whoever -

(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains -

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602 (n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer if the conduct involved an interstate or foreign communication;

(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United

States and such conduct affects that use by or for the Government of the United States;

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;

(5)(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage;

(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if -

(A) such trafficking affects interstate or foreign commerce; Or (B) such computer is used by or for the Government of the United States;

(7) with intent to extort from any person, firm, association, educational institution, financial institution, government entity, or other legal entity, any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer; shall be punished as provided in subsection (c) of this section.

The statute goes on to list potential penalties for committing the aforementioned offenses, which include imprisonment from 5 to 20 years, as well as a variety of potential fines.

A cursory review of the statute reveals that legislators were attempting to cover a broad array of potential violations via a single, all encompassing statute. For example, while section one focuses upon access to protected (i.e. classified) information contained in government systems and subsequent transmittal to other entities (such as would occur in an espionage case), section two focuses on more traditional hacking involving obtaining information from protected computer systems, and does not necessarily require subsequent transmittal or delivery to other parties. Section three focuses upon illegal access to sensitive systems without adding the "obtaining information" caveat.

"A cursory review of the statute reveals that legislators were attempting to cover a broad array of potential violations via a single, all encompassing statute."

The statute also includes provisions to prosecute issues other than hacking, such as causing damage via "transmission of a program, information, code, or command," which could potentially allow for prosecution of those who knowingly transmit viruses, or those who knowingly launch denial of service attacks against systems.

This Issues Suggested Reading

The Cuckoo's Egg

Tracking a Spy Through the Maze of Computer Espionage

The scenario seems like something out of a work of fiction… yet it is entirely true. Cliff Stoll, an astronomer-turned systems administrator discovers a 75-cent accounting error involving his computer network. Upon investigating, Stoll determines that a hacker utilizing the nickname 'Hunter" has compromised the system, and is using the network as a platform to break into sensitive U.S. government computer systems. After several attempts to involve law enforcement which are less than successful, Stoll sets out on his own to catch the hacker who has compromised his network.

"The Cuckoo's Egg" details Stoll's story in a manner that, according to the Chicago Tribune, is "'Reader Friendly,' even for those who have only the vaguest familiarity with computers." Written in 1989, Stoll's book is an "oldie but a goody," but surprisingly enough, many of the exploits referenced are still being used by hackers to compromise systems today. Computer Crime investigators and system administrators should consider it required reading.

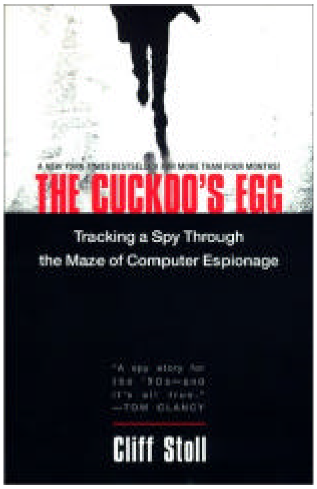
Title:
The Cuckoo's Egg.

Author:
Cliff Stoll

Cost: **$6.99 (paperback)**

ISBN: **0-671-72688-9**

Publisher: **Pocket Books**


A NEW YORK TIMES BESTSELLER FOR MORE THAN FOUR MONTHS!
THE CUCKOO'S EGG
Tracking a Spy Through the Maze of Computer Espionage
"A spy story for the '90s—and it's all true." —TOM CLANCY
Cliff Stoll

A Publication of the DCIS Northeast Field Office

Defense Criminal Investigative Service
Northeast Field Office
10 Industrial Highway, Bldg. G, Mail Stop 75
Lester, PA 19113

Phone: (610) 595-1900
Fax: (610) 595-1934

Send comments to: Jives@dodig.osd.mil

We're on the Web!
www.dodig.osd.mil/dcis/dcismain.html

The Defense Criminal Investigative Service

"Protecting America's War fighters"

The Defense Criminal Investigative Service is the investigative arm of the U.S. Department of Defense, Office of the Inspector General. As such, DCIS investigates criminal, civil, and administrative violations impacting the Defense Department. Typically, DCIS investigations focus upon computer crime involving U.S. military and civilian DoD systems, contract procurement fraud, bribery and corruption, health care fraud, antitrust investigations, export enforcement violations, environmental violations, major thefts of DoD property, and other issues that impact the integrity and effectiveness of the U.S. Department of Defense.

If you encounter issues that impact the U.S. Department of Defense, please call the DCIS office within your region.

***DCIS Northeast Field Office*.**
10 Industrial Hwy., Bldg. G
Lester, PA 19113
Phone: (610) 595-1900
Fax: (610) 595-1934

DCIS Boston Resident Agency
Rm. 327, 495 Summer Street
Boston, MA 02210
Phone: (617) 753-3044
Fax: (617) 753-4284

DCIS Hartford Resident Agency
525 Brook Street, Suite 205
Rocky Hill, CT 06067
Phone: (860) 721-7751
Fax: (860) 721-6327

DCIS New Jersey Resident Agency
Wick Plaza 1, 100 Dey Pl., Ste. 102
Edison, NJ 08817
Phone: (732) 819-8455
Fax: (732) 819-9430

DCIS New York Resident Agency
One Huntington Quad, Suite 2C01
Melville, NY 11747
Phone: (516) 420-4302
Fax: (516) 420-4316

DCIS Pittsburgh Post of Duty
1000 Liberty Ave., Ste. 1310
Pittsburgh, PA 15222
Phone: (412) 395-6931
Fax: (412) 395-4557

DCIS Syracuse Resident Agency
441 S. Selina St., Ste. 304
Syracuse, NY 13202
Phone: (315) 423-5019
Fax: (315) 423-5099